

REMARKS

Upon entry of this amendment, claims 1, 2 and 11-26 are all the claims pending in the application. Claims 3-10 have been canceled by this amendment, and claims 15-26 have been added as new claims. No new matter has been added.

I. Claim Rejections under 35 U.S.C. § 102

Claims 1, 3, 5 and 13 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Kimura (US 2001/0048744).

Claim 1, as amended, recites the features of a receiving section for receiving, from the another communication device, an authentication request including device information by which the another communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted; a transmission section for transmitting an authentication response including information indicative of verification or non-verification of the authentication with the another communication device in accordance with the result input to the input section; and an authentication section for, when the information included in the authentication response is indicative of verification of the authentication, performing key exchange with the another communication device using the device information included in the authentication request and the information included in the authentication response.

Applicants respectfully submit that Kimura does not disclose or suggest the above-noted combination of features recited in claim 1.

Regarding Kimura, Applicants note that this reference discloses an authentication procedure that takes place between an access point device and a mobile station (see Fig. 2). In this regard, as explained in Kimura, this procedure starts with mobile station MT1 sending an authentication request message 1 to the access point device 18 for initiating authentication by the Shared Key Authentication method (see paragraph [0038]). After receiving the authentication request message 1, the access point 18 performs a numerical operation by using the Initialization Vector and Secret Key values as the parameters, so as to obtain a 128-octet uniquely determined Challenge Text value, and sends an authentication response message 1 including this value to the mobile station MT1 (see Fig. 2 and paragraph [0039]).

Next, as disclosed in Kimura, the mobile station MT1 receives the authentication response message 1, and ciphers the included Challenge Text value by using the Shared Secret Data and Initialization Vector as the parameters (see paragraph [0040]). The resulting value and the Initialization Vector are included in an authentication request message 2, which is returned to the access point device 18 (see Fig. 2 and paragraph [0040]).

Upon receiving the authentication request message 2, the access point 18 decodes the received ciphered Challenge Text value based on the Initialization Vector which is received concurrently and the Shared Secret Data which is known in advance (see paragraph [0040]). The result is compared with the original Challenge Text value, and if identical, the access point 18 executes the procedure of AP authentication processing 3 (see paragraph [0040]).

Based on the foregoing description, Applicants note that in Kimura, in order to perform the above-noted Shared Key Authentication method, it is necessary that the Initialization Vector,

the Secret Key, and the Shared Secret Data be stored in advance.

In contrast, according to claim 1, Applicants note that because the key exchange between the communication devices is performed using the device information included in the authentication request and the information included in the authentication response, it is not necessary to store such information in advance.

In view of the foregoing, Applicants respectfully submit that Kimura does not disclose, suggest or otherwise render obvious the above-noted combination of features recited in amended claim 1 of a receiving section for receiving, from the another communication device, an authentication request including device information by which the another communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted; a transmission section for transmitting an authentication response including information indicative of verification or non-verification of the authentication with the another communication device in accordance with the result input to the input section; and an authentication section for, when the information included in the authentication response is indicative of verification of the authentication, performing key exchange with the another communication device using the device information included in the authentication request and the information included in the authentication response.

Accordingly, Applicants respectfully submit that claim 1 is patentable over the cited art, an indication of which is kindly requested.

Regarding claim 13, Applicants note that this claim has been amended so as to recite the features of a first communication device transmitting an authentication request including device information by which the first communication device is capable of being determined to be a source to the second communication device; the second communication device transmitting an authentication response including information indicative of verification or non-verification of the authentication with the first communication device in accordance with the input result; and the first communication device and the second communication device performing key exchange with each other using the device information included in the authentication request and the information included in the authentication response when the information included in the authentication response is indicative of verification of the authentication.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Kimura does not disclose, suggest or otherwise render obvious the above-noted features recited in claim 13. Accordingly, Applicants submit that claim 13 is patentable over the cited prior art, an indication of which is kindly requested.

II. Claim Rejections under 35 U.S.C. § 103(a)

A. Claims 2, 4, 6, 8, 10-12 and 14 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kang et al. (US 7,096,352) in view of Kimura (US 2001/0048744).

Regarding claim 2, Applicants note that this claim has been amended herein so as to recite the features of a transmission section for transmitting an authentication request including device information indicative of the communication device to the another communication device;

a receiving section for receiving, from the another communication device, an authentication response corresponding to the authentication request and including device information by which the another communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted; and an authentication section for executing processing of verifying or not verifying the authentication with the another communication device in accordance with the result input to the input section, and for, when the result is indicative of verification of the authentication, further performing key exchange with the another communication device using the device information included in the authentication request and the authentication response.

Applicants respectfully submit that Kang and Kimura do not teach or suggest at least the above-noted combination of features recited in amended claim 2.

First, with respect to Kang, Applicants note that this reference discloses a handshake process which utilizes a shared secret value that is stored by a client and a server, respectively, wherein the shared secret value is preferably a pre-master secret (see col. 2, lines 60-63). In this regard, as explained in Kang, the handshake process involves the server generating a master secret based on the shared pre-master secret, and generating a key block based on the generated master secret (see col. 3, lines 29-33). Further, as explained in Kang, the last key value for use in encryption and decryption algorithms is generated from the key block (see col. 3, lines 43-45).

Based on the foregoing description, Applicants note that in Kang, in order to generate the key block, which is utilized to generate the last key value, it is necessary that the shared pre-

master key be stored in advance.

In contrast, according to claim 2, Applicants note that because the key exchange between the communication devices is performed using the device information included in the authentication request and the information included in the authentication response, it is not necessary to store such information in advance.

In view of the foregoing, Applicants respectfully submit that Kang does not disclose, suggest or otherwise render obvious the above-noted combination of features recited in amended claim 2 of a transmission section for transmitting an authentication request including device information indicative of the communication device to the another communication device; a receiving section for receiving, from the another communication device, an authentication response corresponding to the authentication request and including device information by which the another communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted; and an authentication section for executing processing of verifying or not verifying the authentication with the another communication device in accordance with the result input to the input section, and for, when the result is indicative of verification of the authentication, further performing key exchange with the another communication device using the device information included in the authentication request and the authentication response.

Second, with respect for Kimura, Applicants respectfully submit that Kimura does not disclose or suggest the above-noted features recited in claim 2 for at least similar reasons as

discussed above with respect to claim 1.

In view of the foregoing, Applicants respectfully submit that the Kang and Kimura do not teach, suggest or otherwise render obvious at least the above-noted combination of features recited in amended claim 2. Accordingly, Applicants submit that claim 2 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 11, Applicants note that this claim has been amended so as to recite that a first communication device includes: a transmission section for transmitting an authentication request including device information by which the first communication device is capable of being determined to be a source to the second communication device; a receiving section for receiving, from the second communication device, an authentication response corresponding to the authentication request and including device information indicative of verification or non-verification of the authentication with the first communication device, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted; and an authentication section for, when the device information included in the authentication response is indicative of verification of the authentication, further performing key exchange with the second communication device using the device information included in the authentication request and the authentication response; and a second communication device that includes: a receiving section for receiving the authentication request from the first communication device, and for monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted; a transmission section for transmitting the authentication response in accordance with the result

input to the input section; and an authentication section for, when the device information included in the authentication response is indicative of verification of the authentication, performing key exchange with the first communication device using the device information included in the authentication request and the authentication response.

For at least similar reasons as discussed above with respect to claims 1 and 2, Applicants respectfully submit that Kang and Kimura do not teach, suggest or otherwise render obvious the above-noted combination of features recited in claim 11. Accordingly, Applicants submit that claim 11 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 12, Applicants note that this claim has been amended so as to recite that a first communication device includes: a transmission section for transmitting an authentication request including device information indicative of the first communication device to the second communication device; a receiving section for receiving, from the second communication device, an authentication response corresponding to the authentication request and including device information by which the second communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted; and an authentication section for, when the result is indicative of verification of the authentication, further performing key exchange with the second communication device using the device information included in the authentication request and the authentication response; and a second communication device that includes: a receiving section for receiving the authentication request from the first communication device, and monitoring and determining whether or not the authentication

request is changed by an unspecified third party while being transmitted; a transmission section for transmitting the authentication response corresponding to the authentication request to the first communication device; and an authentication section for, when the authentication is verified by the first communication device, performing key exchange with the first communication device using the device information included in the authentication request and the authentication response.

For at least similar reasons as discussed above with respect to claims 1 and 2, Applicants respectfully submit that Kang and Kimura do not teach, suggest or otherwise render obvious the above-noted combination of features recited in claim 12. Accordingly, Applicants submit that claim 12 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 14, Applicants note that this claim has been amended so as to recite the features of a first communication device transmitting an authentication request including device information indicative of the first communication device to the second communication device; a second communication device receiving the authentication request from the first communication device, and monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted; the second communication device transmitting an authentication response corresponding to the authentication request and including device information by which the second communication device is capable of being determined to be a source to the first communication device; and the first communication device and the second communication device performing key exchange with each other using the device information included in the authentication request and the authentication response when the result is

indicative of verification of the authentication.

For at least similar reasons as discussed above with respect to claims 1 and 2, Applicants respectfully submit that Kang and Kimura do not teach, suggest or otherwise render obvious the above-noted combination of features recited in claim 14. Accordingly, Applicants submit that claim 14 is patentable over the cited prior art, an indication of which is kindly requested.

B. Claims 7 and 9 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kimura (US 2001/0048744) in view of Kang et al. (US 7,096,352).

Regarding this rejection, as noted above, claims 7 and 9 have been canceled by this amendment.

III. New Claims

As noted above, new claims 15-26 have been added by this amendment.

Regarding these new claims, Applicants note that claims 15 and 17 depend from claim 1; claims 16 and 18 depend from claim 2; claims 19 and 21 depend from claim 11; claims 20 and 22 depend from claim 12; claims 23 and 25 depend from claim 13; and claims 24 and 26 depend from claim 14. Accordingly, Applicants submit that claims 15-26 are patentable at least by virtue of their dependency for the reasons discussed above.

IV. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Applicants hereby petition for any extension of time which may be required in connection with this communication, and any required fee, except for the Issue Fee, and authorize the Commissioner to charge any such required fee to Deposit Account No. 23-0975.

Respectfully submitted,

Yibo ZHANG et al.

By: Kenneth W. Fields
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/krq
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 21, 2009